

ITS Technical Bulletin 175

CONTROL-M SECURITY DEFINITIONS

Issued Date: March 3, 1994
Effective Date: March 8, 1994
Section/Groups:
Submitted By:
Approved By: Dave Jeffs

Extended Security Definitions for Control-M

Correct Copy:

Please disregard incorrect copy of this Bulletin sent out previously today (March 3, 1993).

General Information:

Technical Bulletin 174 on December 16, 1993 described the basic security definition mode for Control-M. To achieve a more flexible security environment under Control-M 'Extended' security definitions will soon be implemented for Schedule Owners. The information in this bulletin supersedes that in section 3 of the previous Bulletin.

1. Schedule Owners

Each Control-M schedule definition has an "OWNER" field that refers to the ACF2 LogonID that Control-M uses to submit the job when it is scheduled. This ACF2 LogonID record must be defined with the RESTRICT and SUBAUTH attributes as well as a SOURCE(STCINRDR) and PROGRAM(CONTROLM). These attributes will allow the logonid to enter the system without supplying a password and ensure that the system will allow this logonid to access the system through the authorized program (CONTROL M) and the authorized source (internal reader). JCL for jobs submitted through Control-M must not have LogonIDs or Passwords cards coded.

In order for Control-M to ensure that only authorized people can manipulate jobs which contain these restricted LogonIDs, certain ACF2 resource rules will be checked by Control-M before any function is performed. The following table describes which rules will be checked before certain functions are performed:

- Browse Job Sysout
- Show Job Statistics
- Zoom Job
- Show Job Log
- Hold Job
- Free Job
- Rerun Job
- Confirm Job

Change Job
Change Job Priority
Delete Job
Edit Job JCL
\$\$JOBORD.I2.owner
\$\$JOB1SYS.I2.owner
\$\$JOB1STA.I2.owner
\$\$JOB1ZOO.I2.owner
\$\$JOB1LOG.I2.owner
\$\$JOB2HLD.I2.owner
\$\$JOB2FRE.I2.owner
\$\$JOB2RRN.I2.owner
\$\$JOB2CNF.I2.owner
\$\$JOB3CHA.I2.owner
\$\$JOB3PRI.I2.owner
\$\$JOB3DEL.I2.owner
\$\$JOB3EDI.I2.owner

The access granted by these ACF2 resource rules allows ITS and agency administrators to define who is able to manipulate jobs that run under the authority of the agencies' Batch LogonIDs. There must be a separate set of the above ACF2 rules for each OWNER (ACF2 LogonID). Currently, these rules are all next-keyed to a common rule with a key of the LogonID. Under the future release of ACF2 more levels and functionality of next-keys will be available.

The owner of these Control-M resources will be the person responsible for the specific Batch LogonID. Security access to these Control-M resources will be administered by each agency's security personnel.

The following rule line will be required in each \$\$JOBORD.owner rule:

UID(ASITSYOP) ALLOW DATA(CONTROL-M STARTED TASKS)

This rule will allow the Control-M monitor and its associated tasks to submit job-streams with this logonid.